Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
NetOps, here we come! Facing some hard questions	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Signal Center of Excellence,Army Communicator,Signal Towers (Building 29808), Room 713,Fort Gordon,GA,30905-5301**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**2**	

NetOps, here we come!

Facing some hard questions

By CW5 Todd M. Boudreau

If your most savvy adversary is currently using your highways and byways to transport goods, they are stealing from you. Although they may possess the ability to disrupt your motorways and/or destroy your roads, to do so would negatively affect their own operations.

However, if there was a shift that caused the adversary to value stopping our use of the roadways more than their use of them to transport stolen goods, would we be prepared to defend them… every one of them?

So what does a conversation that may be best suited for Homeland Defense have to do with cyber defense? Change the environment and the scenario remains constant. Open source intelligence acknowledges that our communications platforms and transport systems (i.e., data highways) are under constant attack through probes and malware every day. Much of what we see is cannon fodder. However, unmitigated it drastically increases the noise floor making it possible for a skilled adversary to surreptitiously enter our networks, gain a foothold into our information systems, and begin Computer Network Exploitation actions such as exfiltrating data.

If, however, there is a change in relations with said adversary due to a political decision or kinetic contest somewhere in the world, said adversary could easily shift from CNE operations to a Computer Network Attack posture. With the criticality of our technology systems to our combat operations, are we ready to operate while an adversary attempts to manipulate data and/or to disrupt the operations of, deny our uninterrupted access to, and/or destroy our information systems?

Few today would argue that defending our communications systems and the critical information within them is more than a full-time job; but not so many understand that everyone has a level of responsibility.

Just as a reminder, take a moment to remember (or imagine for those who did not live the days of Mobile Subscriber Equipment and Tri-Service Tactical; MSE and TRI-TAC respectively, the magnitude of barriers our opponents faced in the days of MSE and TRI-TAC to gain entrance into our military networks, just under the perspective of equipment, architecture, and investment. The equipment used under the MSE and TRI-TAC programs was proprietary; Commercial-off-the-Shelf equipment had not yet been popularized in tactical transport services.

The architecture, even though it included meshed networks, was based off a circuit switched paradigm which afforded some level of Low-Probability-of-Interception. So, there was a substantial investment required to attack such a communications system.

Those with intent to attack our networks did not necessarily pose a threat since they did not also possess knowledge of vulnerabilities and the capability to exploit said vulnerabilities. As the equipment was mostly proprietary, an adversary would need to obtain and reverse engineer our equipment, and then identify vulnerabilities; then such a foe would need to create or exploit the opportunity to intercept a circuit switched, encrypted, timed trunk dependant communications link – all huge barriers in themselves.

Today, however, over ninety-percent of our military communications infrastructure, platforms, and programs are COTS; software and equipment available to anyone. Our current TCP/IP architecture was developed for transparency, interoperability, and technology insertion; not necessarily with security in mind. As vulnerabilities are identified they are oftentimes posted in the open for all to see. Capability sets to attack and exploit such vulnerabilities are easily obtainable.

So the substantial investment required to attack has been significantly reduced, creating a converse and exponentially increased investment required to defend; the Federal Government reportedly spent $12B in IT Security in 2010; 15% of its total IT spending.

Those with intent to harm our military communications networks and to exploit and/or

(Continued on page 14)

How well are we prepared to face a peer, or even a near-peer adversary in our cyberspace?

(Continued from page 13)

manipulate critical information merely need to know where to look to find a virtual cornucopia of attack capabilities. With $50k, anyone with inclination and desire can hire a botnet and launch a distributed denial-of service attack; similar to those that struck South Korea, Georgia, Estonia, and yes, even segments and portions of the United States.

While in the past, the technical complexity required of the attack capability was to our advantage, today various aspects of technology, to include its availability, have added to the necessary technical complexity of the defense capability. For example, the average low-tech, yet often effective, attack toolset is in the order of hundreds of lines of code, whereas the average defense toolset is in the order of millions.

What is needed is the ability to invoke a machine-on-machine response in order to counter attacks made at network-speed. And while we have made great strides toward that end, a myriad of obstacles have yet to be breached. To that end, we need everyone involved in the defense of our communications networks and systems. I could go on and talk about the need for the common user to understand cyberspace as an operational domain and to be able to make parallel connections such as viewing emails from unknown recipients as possible unexploded ordinance or cyber incoming. I could also spend time talking about how important it is for our senior leaders to understand the imminence of the threat and consciously measure the importance of our essential cyber terrain. However, instead I would like to challenge us, Signaleers, Cyber Warriors, those of us interested enough to read the articles in this *Army Communicator.*

How well are we prepared to face a peer, or even a near-peer adversary in our cyberspace? Beyond establishing an up-armored cyber defensive posture, beyond ensuring all policies and governance has been followed, beyond ensuring all systems are patched and up-to-date, are we prepared to build, manage, and shape our cyberspace to ensure we maintain the advantage when our adversaries have entered and are performing disrupt, deny, destroy operations? When our networks and networked systems, installed, operated, and maintained by us are no longer uncontested operational space, are we ready, prepared, and able to ensure uninterrupted Mission Command Essential Capabilities?

While we are shaping our cyber workforce to include expert defenders who are able to understand the adversaries tactics, techniques, and procedures, response actions, or better yet preemptive response actions within our own LandWarNet requires experts in transport and complex Mission Command systems as well. As I asked in my opening comments, although we have a NetOps construct, are we really conducting, or even able to conduct true Network Operations? Are our experts in transport and routing able to make changes beyond reactive optimizations based on bandwidth demands? Are our experts in establishing data services able to adapt beyond a static model of Mission Command service expectations and out maneuver an aggressive adversary in a contested battle-space? Are we collectively trained, tested, and prepared to conduct NetOps?

Armed with knowledge, actionable intelligence, and a host of tools (both specifically specialized as well as converged such as the Defense Information Systems Agency's Host-Based Security System) our expert cyber defenders hunt for potential adversarial activity used to prepare for CNE and/or CNA activity in order to catch and posture for response actions before any damaging activities can be accomplished. Once anomalous activity is identified and categorized as adversarial, pre-coordinated actions in accordance with an established playbook are initiated. In many cases, such actions will include immediate preemptive transport routing modifications as well as data screening, filtering, and transition to alternate servers.

The cry of this article is for an understood, acknowledged, collectively trained NetOps posture enabling us to make appropriate adaptations to our operational portion of cyberspace in the midst of a peer or near-peer adversary's attempt to deny us freedom of movement, disruption of critical services, and/or manipulation of critical information. Are we there yet? If not, either by design or by necessity…NetOps, here we come.

CW5 Todd M. Boudreau *is the U. S. Army Signal Regiment Chief Warrant Officer.*